AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
INFORMATION ASSOCIATED WITH [iamyoungjudah@gmail.com] [reddymoneypocket@gmail.com] THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE INC.

Case No. 19-mj-279-PJC

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 1591(a)(1), 1591(a)(2), and 1591(b)(1)	**Sex Trafficking by Force, Fraud and Coercion**
18 U.S.C. § 1591(d)	**Attempted Obstruction of Sex Trafficking Enforcement**
18 U.S.C. § 1513(b)(2)	**Retaliating Against a Victim and Causing Bodily Harm**
18 U.S.C. § 2421(a)	**Transporting Individual for Prostitution**
18 U.S.C. § 2421A(a)	**Online Promotion and Facilitation of Prostitution**

The application is based on these facts:

See Affidavit of Justin Oxford, attached hereto.

☑ Continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than 30 _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Justin Oxford, TPD-FBI Task Force Officer
Printed name and title

Sworn to before me and signed in my presence.

Date: 12/26/19

Judge's signature

City and state: Tulsa, OK Tulsa, Oklahoma

Paul J. Cleary, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH **[iamyoungjudah@gmail.com] [reddymoneypocket@gmail.com]** THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC.	Case No. 19-mj-279-PJC **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Justin D. Oxford, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with Google accounts [iamyoungjudah@gmail.com] and [reddymoneypocket@gmail.com] (herein referred to "subject accounts") that is stored at premises controlled by Google LLC, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 9043, USA. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am an FBI Task Force Officer with the Tulsa Police Department and have been since March of 2019. I have been a police officer for over 12 years. I received a bachelor's degree in organizational leadership from the University of Southern Nazarene in Bethany,

Oklahoma. In August of 2016, I was assigned to the Special Investigations Division, Vice unit. While assigned to the Vice Unit, I worked in an undercover capacity investigating street level narcotics, illegal gambling, prostitution, pandering, and human trafficking crimes. In March of 2017, I completed a 36-hour Vice and Human Trafficking Investigations school in Daytona, Florida. In July of 2017, I completed the two-week Basic Narcotics Investigator School hosted by the United States Drug Enforcement Administration training staff. Furthermore, I served on the U.S. Attorneys Human Trafficking Task Force from August 2016- March 2019. I regularly attended and presented material at the Office of The Attorney General of Oklahoma at the Human Trafficking Intelligence meetings in Oklahoma City.

3. I have been involved in numerous, prostitution, pandering, and human trafficking investigations. This experience includes physical surveillance, participation with other agents in the consensual and court-authorized electronic surveillance of human trafficking and pandering activities, the execution of evidentiary search warrants, and search warrants for documents and records related thereto.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 USC 1591, 18 USC 1591(d), 18 USC 1512, 18 USC 2422, 18 USC 2422A, and 18 USC 1513 have been committed by Ramar Palms. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

PROBABLE CAUSE

6. On November 20, 2018, I was working in a plain clothes capacity and conducting prostitution investigations using websites known for soliciting prostitution, such as www.cityxguide.com. I discovered an advertisement on cityxguide.com for a "Lunch Break Special." The photographs of the female in the advertisement appeared to be an under-age juvenile. I sent a text message to the phone number associated with the advertisement, asking if she still had her $100.00 Quick Visit Special (Prostitution deal lasting less than 15 minutes.). The female confirmed she was available and directed me to the Peoria Inn Motel, located at 1347 E. Skelly Drive, room #220 in Tulsa, Tulsa County, Oklahoma.

7. When I arrived at the Peoria Inn Motel I parked near the office. I exited my vehicle and walked across the parking lot to the stairwell leading up to room #220. As I approached the stairwell, I noticed a black male, who was later identified as, Ramar Palms sitting in an SUV at the bottom of the stairs. Palms watched me walk up the stairs and to the room.

8. I knocked on the door to room #220 and was invited in the room by a white female later identified as Mary Walton. Once inside the room, I placed $100.00 on the night stand and Walton began getting undressed. I asked Walton if there was anything she did not do. Walton replied, "not really." I asked Walton if we could start with oral sex in which she agreed to the sex act. I then identified myself as a Tulsa Police Officer and told her she was under arrest for Engaging in Prostitution. I directed the arrest team to detain Palms, who was still sitting in the SUV at the bottom of the stairs.

9. I asked Walton for identification. Walton told me her Oklahoma Drivers license was stored in her purse in the night stand. I retrieved Walton's purse from the night stand, which contained a black .380 hand gun, Walton's Oklahoma Drivers License, Walton's concealed carry

permit, Palm's Oklahoma Identification Card, and three condoms. Sgt. Todd Evans picked up Walton's cell phone which was open to a message from Palms letting her know I had arrived and I looked "kool," meaning he did not think I was a law enforcement officer.

10. Walton stated Palms was collecting her money from prostitution deals and providing security during the dates. Palms guided Walton through posting advertisements for prostitution on websites known for prostitution. Palms would transfer money to Walton's bank account to pay for prostitution advertisements in an effort to distance himself from the criminal aspect of the prostitution. Palms would threaten Walton if she did not do at least five prostitution dates a night. Palms would slap Walton with his knuckles and rings on his fingers if she did not get enough prostitution dates. Palms provided security during the prostitution dates by making Walton text him when the client had arrived and when the prostitution deal was completed. If a client stayed past time Palms would come up to the room and confront the client. Palms provided condoms for Walton to use during the prostitution deals by getting free condoms at the health department.

11. Walton told Officers she had first met Palms while working as a bartender at the Ambassador Lounge in Tulsa. Shortly after meeting Palms, Walton was invited by Palms to take a road trip to Louisiana. Walton and Palms took a road trip to Louisiana in Walton's car. Walton stated while driving on a desolate stretch of highway in Louisiana, Palms stopped the car, turned to Walton and said, "you know I'm a pimp?" Palms told Walton that she is going to quit her job and work for him as a prostitute. Palms subsequently drove Walton to a hotel in Louisiana where he engages in degrading sexual acts with Walton. Palms then transports Walton across state lines to Houston, Texas to a second hotel where Walton began working as a prostitute for Palms. Palms transported Walton on two subsequent trips to Louisiana, Texas, and

Oklahoma for the purpose of prostitution. It was on that trip that Palms informed Walton of the website cityxguide.com, which he had previously used to post ads for prostitution. He told her to keep the website a secret, as not many people in the Tulsa area knew about it. Palms initially posted prostitution ads for Walton, before delegating the responsibility to her, while still informing her of the prices and content to put on the ads. Palms also had Walton post prostitution ads on a website called whatsyourprice.com, which allows women to sell "dates" to bidders, and is a known front for prostitution.

12. Palms cellular phone was seized as evidence after his arrest on November 20, 2019. A cellebrite forensic examination was conducted on the cellular device and a report was generated. There were several text messages from Palms to Walton, directing Walton on prices, times, and places for prostitution acts to be conducted. In several messages, Palms directs Walton to place advertisements for prostitution for herself and at least two other women on the website www.cityxguide.com and what content to put on the advertisements. Recovered internet history for a twenty day period shows Palms visited the cityxguide website over 500 times. Palms also visited the members section of whatsyourprice.com over 130 times. Dozens of screenshots of cityxguide ads were also found in the phone. Emails from whatsyourprice were found in the iamyoungjudah@gmail.com and reddymoneypocket@gmail.com accounts that were being used on the phone. Emails from other dating sites that are frequently used as fronts for prostitution were also found.

13. After Palms' November 20 arrest, he was released on bond. He continued to force Walton to engage in prostitution, facilitated by the internet. Investigators recently located a Whatsyourprice.com advertisement of Walton that was posted on December 9, 2018. Investigators also discovered a December 2019 Whatsyourprice.com advertisement for Kristin

Shepherd, a girlfriend Palms and mother of one of his children. Shepherd was present every day of Palms' December 2-5 trial, but investigators uncovered jail messages between the two that discuss Shepherd still being able to "work" despite her attendance at the trial.

14. On January 9, 2019, Walton meet Palms at the Market Pub location at 5058 S. 79th East Avenue. While hanging out at the Market Pub there was an argument between Walton and two females, Sasha Hawkins and Hannah McDonnell. Walton and Palms walked to the parking lot, at which point Palms grabbed Walton by the throat and threw her on the ground. Palms threw Walton back down to the ground two more times as she tried to stand up. Palms punched Walton in the face while yelling "bitch, I know you are working with the police! I'm gonna kill you, if you don't get in the truck!" Walton stated patrons from the bar were outside and broke up the altercation preventing Palms from dragging her into the vehicle. Walton told investigators Palms stole her .380 hand gun and her debit cards from her purse before leaving. I met with Walton on January 10, 2019 to file a Domestic Violence Report and observed injuries on Walton consistant with her statement about the altercation.

15. Palms was indicted in the Northern District of Oklahoma for Sex Trafficking by Force, Obstruction of Sex Trafficking Enforcement, and Retaliation Against a Victim in June 2019. A December 2-5 jury trial resulted in a mistrial, with retrial set for January 21. A December superseding indictment charged Palms with Transportation for Prostitution and Online Promotion and Facilitation of Prostitution.

BACKGROUND CONCERNING EMAIL

16. In my training, experience, and research, I have learned e-mail providers such a Google usually maintain the following records and information with respect to subscriber accounts:

a. *E-mail content.* In general, any e-mail (which can include attachments such as documents, images, and videos) sent to or from a subscriber's account, or stored in draft form in the account, is maintained on the e-mail providers' servers unless and until the subscriber deletes the e-mail. If the subscriber does not delete the e-mail, it can remain on the provider's servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on the provider's servers for a certain period of time.

b. *Address Book.* E-mail providers usually also allow subscribers to maintain the equivalent of an address book, comprising e-mail addresses and other contact information of other e-mail users.

c. *Device Information.* E-mail providers can collect and maintain information identifying devices (including both computers and mobile devices) used to access accounts, including, for example, device serial number, a GUID or Global Unique Identifier, a phone number, MAC addresses, Electronic Serial Numbers, Mobile Electronic Identify Numbers, Mobile Equipment Identifiers, Mobile Identification Numbers, Subscriber Identity Modules, Mobile Subscriber Integrated Services Digital Network Number, International Mobile Subscriber Identifiers, or International Mobile Equipment Identities.

d. *Subscriber and billing information.* The e-mail provider can collect and maintain (typically unverified) identifying information about each subscriber, including, for example, name, username, address, telephone number, and alternate e-mail addresses. The e-mail providers can also maintain records concerning the date on which the account was created, the Internet Protocol address of the user at the time of account creation, the current status of the account (e.g., active or closed), the length of service, and the types of services utilized by the subscriber. Additionally, for paying subscribers, the e-mail provider can also maintain records of the subscriber's means and source of payment, including a credit card or bank account number

e. *Cookie Data.* E-mail providers can use features to track the activity of users of their accounts, including whether or not the user of an account accesses other accounts at the e-mail provider using the same computer. One of the ways e-mail providers accomplish this is by using cookies, a string of characters stored on the user's computer or web browser that is recognized by the e-mail provider when a computer visits its website or logs into an account.

f. *Transactional Information.* The e-mail providers typically retain certain transactional information about the use of an account. This information can include records of login (i.e. session) times and durations and the methods used to connect to the account.

g. *Location History.* E-mail providers can also collect data on the location of their users from their electronic devices. E-mail providers use this information for, among other things, location-based advertising, location-based search results,

embedding location information in photographs and videos taken by the user (known as geo-tagging), navigation through maps and services and related applications, and features that permit users to locate their mobile electronic devices if they lose them.

h. *Customer correspondence.* E-mail providers can also maintain records of any customer service contacts with or about the subscriber, including any inquiries or complaints concerning the subscriber's account.

i. *Preserved and backup records.* E-mail providers can also maintain preserved copies of the foregoing categories of records with respect to an account, for 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. Section 2703(f).

17. In the Affiant's training, experience, and research, Affiant has learned Google also maintains records with respect to other Google services, which it stores in connection with e-mail accounts, which can include, in part, the following:

a. *Google Drive Content.* Google can provide users with a certain amount of free cloud storage, which is currently approximately 15 gigabytes, through a service called Google Drive. Users can purchase a storage plan through Google to store additional content. Users can use their Google Drive to store e-mail, attachments, videos, photographs, documents, and other content "in the cloud," that is online. A user can access content stored on Google Drive by logging into his or her Google account through any computer or other electronic device that is connected to the Internet. Users can also share files stored on Google Drive with others, allowing them to view, comment, and/or edit the files.

b. *Google Docs.* Google can provide users with the ability to write, edit, and collaborate on various documents with other Google users through a service called Google Docs. Users can use Google Docs to create online documents which can be stored on or saved to the user's Google Drive.

c. *Google Photos.* Google can provide users with a certain amount of free storage for photographs, through a service called Google Photos, which allows users to store photographs and videos. Google also retains the metadata-or data that provides information about the data in question, such as the time and date of creation, the author or creator, the means of its creation, the purpose of the data, among other data—for photos and videos that are uploaded to Google, including to Google Photos. This metadata can include what is known as exchangeable image file format (EXIF) data, and can include GPS location information for where a photo or video was taken.

d. *Google Calendar.* Google provides users with an online calendar, in which they can add appoints, events, and reminders, which are synchronized across registered computers and mobile devices. Users can share their calendars with other users, allowing the maintenance of joint calendars.

e. *Google Chats and Google Hangouts content.* Google allows subscribers to engage in "chat" sessions in an instant messaging format with other Google users. Similarly, Google allows users to engage in enhanced chat sessions, called Hangouts, which can permit the sharing of additional content such as videos, sounds, and images. In general, Hangouts content is stored separately from a user's e-mail and chat content.

f. *Location History Data.* Google can maintain recent location data, collected periodically, from mobile devices that are logged into or have used applications or services provided by Google. For example. Google can collect information collected from GPS, or Wi-Fi networks, cell site locations, and mobile networks to estimate a user's location Google applications and services can also allow for location reporting, which allows Google to periodically store and use a device's most recent location data in connection with a Google account.

g. *Google Payments.* Google allows for the storage of payment information associated with a Google Account, including credit cards and bank accounts, and contains information about all transactions made with a Google account, allowing for the payment for goods (such as those purchased through Google Shopping) and bills, among other features.

h. *Chrome Browser and Search History.* Google can store information regarding user Internet browser activity when a Google user is logged into his or her account, which includes logging information about websites viewed by the user, Internet search queries in the Google Internet search engine available at http://www.google.com, and also maintains lists of bookmarks maintained by the user so that he or she can quickly access frequently viewed websites.

EVIDENCE OF CRIMINAL CONDUCT UNDER INVESTIGATION STORED IN CONNECTION WITH E-MAIL ACCOUNTS

18. As explained herein, information stored in connection with an e-mail account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or

alternatively, to exclude the innocent from further suspicion. In Affiant's training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the e-mail provider can show how and when the account was accessed or used. For example, as described above, e-mail providers typically log the Internet Protocol addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

19. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and

other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

20. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

21. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute

evidence of the crimes under investigation because the information can be used to identify the account's user or users.

As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*,

communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

REVIEW OF INFORMATION OBTAINED PURSUANT TO THE WARRANT

1. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to Google LLC, which shall be directed to produce a digital copy of any responsive records to law enforcement personnel. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the Government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence and instrumentalities of the Subject Offenses as specified in Attachment B to the proposed warrant.

2. In conducting this review, law enforcement personnel may use various methods to locate evidence and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all information within the Subject Accounts. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, Affiant knows that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with e-mails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account as it is impossible to know in advance

all of the unique words or phrases investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but do not contain any keywords that an agent is likely searching for.

REQUEST FOR SEALING

3. Affiant respectfully requests this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation. As set forth above, the target(s) of this investigation are known to use computers and electronic communications in furtherance of their activity and thus could easily delete, encrypt, or otherwise conceal such digital evidence from law enforcement were they to learn of the Government's investigation.

4. Based on the forgoing, Affiant requests that the Court issue the proposed search warrant. Because the warrant will be served on Google LLC, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

CONCLUSION

5. Based on the forgoing, I request that the Court issue the proposed search warrant.

6. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google, Inc. Because the warrant will be served on Google, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Justin D. Oxford
FBI Task Force Officer
Tulsa Police Department

Subscribed and sworn to before me on December 26, 2019

Honorable Paul J. Cleary
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant is directed to Google LLC (the "Provider"), headquartered at 1600 Amphitheatre Parkway, Mountain View, California and applies to all content and other information within the Provider's possession, custody, or control associated with the e-mail account iamyoungjudah@gmail.com and reddymoneypocket@gmail.com (the "Subject Accounts") from account inception through present.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account listed in Attachment A:

1. *E-mail Content.* All e-mails sent to or from, stored in draft form in, or otherwise associated with the Subject Accounts, including all message content, attachments, and header information (specifically including the source and destination addresses associated with each e-mail, the data and time at which each e-mail was sent, and the size and length of each e-mail), limited to items sent, received, or created between February 26, 2019 and present;
2. *Address book information.* All address book, contact list, or similar information associated with the Subject Accounts.
3. *Google services information.* The files and contents with the account related to Google services, including Google Drive, Google Docs, Google Photos, Google Calendar, Google Chats, Google Hangouts, Google Photos, Web and Search History, and Google Payments.
4. *Subscriber and payment information.* All subscriber and payment information regarding the Subject Accounts, including but not limited to name, username,

address, telephone number, alternate e-mail addresses, registration IP address, account creation date, account status, length of service, types of services utilized, means and source of payment, and payment history.

5. *Search and web history records.* All records relating to web and application activity history (including search terms), device information history, and location history.

6. *Device information.* Any information identifying the device or devices used to access the Subject Accounts, including a device serial number, a GUID or Global Unique Identifier, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identify Numbers ("MEIN), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"), and any other information regarding the types of devices used to access the Subject Accounts.

7. *Information Regarding Linked Accounts, Including Linked by Cookie.* Any information identifying accounts that are associated or connected to the Subject Accounts, including specifically by cookie, Google Account ID, Android ID, or other account or device identifier (the "Linked Accounts").

    a. The following information regarding the customers or subscribers of the Linked Accounts:

1. Names (including subscriber names, user name, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
3. Local and long distance telephone connection records;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol addresses and port numbers) associated with those sessions;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses);
7. Other subscriber numbers or identities (including the registration Internet Protocol address); and
8. Means and source of payment for such service (including any credit card or bank account number) and billing records.

8. *Location Data.* All location data associated with the Subject Accounts, including GPS data, cell site/cell towner triangulation/trilateration, and Wi-Fi location, including the GPS coordinates and dates and times of all location recordings.
9. *Transactional records.* All transactional records associated with the Subject Accounts, including any IP logs or other records of session times and durations.
10. *Customer correspondence.* All correspondence with the subscriber or others associated with the Subject Accounts, including complaints, inquiries, or other contacts with support services and records of actions taken.

11. *Preserved or backed up records.* Any preserved or backup copies of any of the foregoing categories of records, whether created in response to a preservation request issued pursuant to 18 U.S.C. Section 2703(f) or otherwise.

Google is further ordered to disclose the above information to the Government within 14 days after service of this warrant.

II. Information to be seized by the government

1. All information described above in Section I that constitutes evidence and/or instrumentalities of violations of Title 18, United States Code, Sections 1591(sex trafficking), 2421A (online promotion and facilitation of prostitution), and 2421 (transportation for prostitution), including information pertaining to the following matters:

a. E-mail communications relating to the offenses;

b. Any information related to the offense;

c. Information identifying the user or the location of the user of the Subject Accounts, and the individual involved in the Subject Offenses, including photographs or videos depicting the user of the Subject Accounts, communications with individuals that the user of the Subject Accounts trusts, which reveal his/her identity to include information that can be used to ascertain his/her identity, such as travel information or receipts for online purchases or other communications with social network websites or third party service providers;

d. Communications of the user of the Subject Accounts with co-conspirators and others about the Subject Offenses, and communications and other data identifying such co-conspirators;

e. Communications and documents concerning the wiring or transferring of funds between bank accounts in relation to prostitution;

f. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

g. Information regarding the registration of other e-mail accounts, computer servers, or other computer network infrastructure, including servers and Internet domains, or online communications facilities, and payment for such online facilities or services; and

h. Evidence concerning any other online accounts or any computer devices where evidence falling within the foregoing categories could be stored, including any passwords or encryption keys needed to access such evidence.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google, Inc., and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google, Inc. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, Inc., and they were made by Google, Inc. as a regular practice; and

b. such records were generated by Google, Inc.'s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google, Inc. in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, Inc., and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature